



Modifikasi Sistem Kripto ElGamal Hasil Konstruksi Marc Joye Menggunakan General Linear Group

¹Maxrizal, ²Maya Saftari, ³Eza Budi Perkasa, ⁴Devi Irawan

¹Sistem Informasi, STMIK Atma Luhur

^{2,3} Teknik Informatika, STMIK Atma Luhur

⁴Mahasiswa S2 Ilmu Komputer, Universitas Budi Luhur

maxrizal@atmaluhur.ac.id

Abstrak

Pada era revolusi teknologi 4.0, transformasi big data yang dikumpulkan melalui internet pada segala bidang kehidupan (The Internet of Things) merupakan suatu keharusan. Akan tetapi internet bukanlah media komunikasi yang cukup aman karena rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengakses informasi tersebut.

Kriptografi merupakan salah satu bidang keilmuan untuk menjaga keamanan informasi. Salah satu sistem kriptografi yang masih digunakan sampai saat ini adalah sistem kriptografi ElGamal yang diperkenalkan oleh Taher ElGamal. Pada sistem kriptografi ElGamal klasik dan sistem kriptografi modifikasi ElGamal yang dikonstruksikan oleh Marc Joye, masing-masing sistem kriptografi ini menggunakan konsep bilangan bulat (integer). Fakta ini memotivasi suatu ide untuk menggantikan konsep bilangan bulat (integer) menjadi suatu matriks yang berukuran $n \times n$ yang dinamakan dengan General Linear Group. Keunggulan dari sistem kriptografi yang diusulkan adalah terdapat ruang plaintext yang lebih besar dari sistem sebelumnya, sehingga ciphertext menjadi lebih acak dan keamanan pengiriman data menjadi lebih aman.

Penelitian ini merupakan jenis penelitian studi literatur. Sedangkan tujuan dari penelitian ini adalah untuk memodifikasi sistem kriptografi ElGamal hasil konstruksi Marc Joye menggunakan konsep General Linear Group sehingga dihasilkan suatu modifikasi sistem kriptografi ElGamal usulan yang lebih aman dari sistem kriptografi ElGamal hasil konstruksi Marc Joye. Untuk itu, pada makalah ini diusulkan suatu modifikasi yang menggabungkan keunggulan dari sistem kriptografi ElGamal yang dikonstruksikan oleh Marc Joye dan prinsip general linear group. Hasil menunjukkan bahwa modifikasi sistem kriptografi ElGamal yang dihasilkan harus menggunakan general linear khusus yaitu matriks-matriks sirkular yang invertible atas modulo p .

Kata kunci: modifikasi ElGamal, General Linear Group, ElGamal menggunakan General Linear Group.

Abstract

In the era of technological revolution 4.0, the transformation of big data collected through the internet in all areas of life (The Internet of Things) is a must. However, the internet is not a communication medium that is quite safe because it is prone to tapping information by parties who are not entitled to access the information.

Cryptography is one of the scientific fields to maintain information security. One of the cryptosystems that are still used today is the ElGamal cryptosystem introduced by Taher ElGamal. In the classic ElGamal cryptosystem and ElGamal's modified cryptosystem constructed by Marc Joye, each of these cryptosystems uses the concept of integers. This fact motivates an idea to replace the concept of integers into an $n \times n$ -sized matrix named General Linear Group. The advantage of the cryptosystem that is

proposed is that there is a plaintext space that is larger than the previous system, so the ciphertext becomes more random and the security of data transmission becomes safer.

This research is a type of literature study. While the purpose of this study is to modify the ElGamal cryptosystem from Marc Joye's construction using the General Linear Group concept so that a modified ElGamal cryptosystem is produced which is safer than the ElGamal cryptosystem produced by Marc Joye. For this reason, we propose a modification that combines the advantages of the ElGamal cryptosystem constructed by Marc Joye and the general linear group principle. The results show that the modification of the resulting ElGamal cryptosystem must use a special general linear, namely circulatory matrices that are invertible to modulo p .

Keywords: *ElGamal modification, General Linear Group, ElGamal uses the General Linear Group.*

A. Pendahuluan

Pada era revolusi teknologi 4.0, transformasi *big data* yang dikumpulkan melalui internet pada segala bidang kehidupan (*The Internet of Things*) merupakan suatu keharusan. Teknologi internet sangat membantu manusia untuk menjalani kehidupan sehingga menjadi lebih mudah dan lebih bermakna. Akan tetapi internet bukanlah media komunikasi yang cukup aman karena siapapun dapat mengakses dengan mudah sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengakses informasi tersebut.

Kriptografi merupakan salah satu bidang keilmuan untuk menjaga keamanan informasi. Bidang keilmuan ini dibangun pada prinsip penyandian pesan agar tidak terbaca dengan mudah oleh pihak-pihak yang tidak berhak mengakses informasi tersebut. Salah satu sistem kriptografi yang masih digunakan sampai saat ini adalah sistem kriptografi *ElGamal* diperkenalkan oleh Taher *ElGamal* pada tahun 1984 (*ElGamal*, 1985; Joye, 2016; Rao, 2017). Sistem kriptografi *ElGamal* merupakan sistem kriptografi asimetri yaitu pihak penerima dan pihak pengirim informasi memiliki kunci yang berbeda, sehingga meminimalkan proses penyadapan akibat pertukaran kunci yang sama seperti pada sistem kriptografi simetri.

Pada faktanya, sistem kriptografi *ElGamal* telah mengalami banyak modifikasi. Sistem kriptografi ini telah digunakan pada keamanan pengiriman data dengan tipe hybrid antar organisasi (Murakami & Kasahara, 2015). Sistem kriptografi ini juga telah dimodifikasi pada proses enkripsinya agar diperoleh sistem kriptografi modifikasi *ElGamal* yang lebih aman (Fang, Liu, & Wu, 2016; Sharma, Sharma, & Dhakar, 2011; Yang, Chang, Li, & Hwang, 2003). Pada tahap selanjutnya, sistem ini juga telah dikombinasikan dengan konsep kurva eliptik (Boruah & Saikia, 2015; Fu & Chen, 2010) dan telah diterapkan pada struktur bilangan atas lapangan (*field*) dan grup tertentu (Fun & Samsudin, 2018; Mandangan, Yin, Hung, & Hussin, 2014). Selain itu, tipe modifikasi dan ragam sistem kriptografi

ElGamal banyak dikembangkan dalam beberapa tahun terakhir (Bharathi, 2018; Mahalanobis, 2012; Rao, 2017).

Berdasarkan fakta di atas, sistem kriptografi *ElGamal* klasik dan modifikasinya menggunakan konsep bilangan bulat (*integer*), bilangan prima dan sifat istimewa dari modulo untuk menyandikan dan mengacak informasi. Sedangkan pada sistem kriptografi *ElGamal* yang dikonstruksikan oleh Marc Joye, dimodifikasi dengan menambahkan proses verifikasi antara pihak pengirim dan pihak penerima pesan (Joye, 2016). Hasil menunjukkan bahwa sistem kriptografi *ElGamal* yang dikonstruksikan oleh Marc Joye, lebih aman dari pada sistem kriptografi *ElGamal* klasikal dan modifikasinya.

Perhatikan bahwa sistem kriptografi *ElGamal* klasik atau sistem kriptografi *ElGamal* yang dikonstruksikan oleh Marc Joye, menggunakan prinsip bilangan bulat (*integer*). Fakta ini menimbulkan suatu ide untuk menggantikan konsep bilangan bulat menjadi suatu matriks yang berukuran $n \times n$. Berdasarkan (Hartanto, Junia, & Palupi, 2016), matriks-matriks yang digunakan adalah *General Linear Group* yang digunakan untuk memodifikasi sistem kriptografi *RSA* klasik (*RSA**). Hasil menunjukkan bahwa sistem kriptografi *RSA** mempunyai keamanan yang lebih baik daripada sistem kriptografi *RSA* klasik, karena kemungkinan ruang *plaintext* pada sistem kriptografi *RSA** lebih banyak dari pada sistem kriptografi *RSA* klasik (Hartanto et al., 2016). Hasil ini menunjukkan bahwa penggunaan konsep *General Linear Group* jauh lebih aman (signifikan) dari pada penggunaan konsep bilangan bulat (*integer*).

Untuk itu, pada makalah ini diusulkan suatu modifikasi sistem kriptografi *ElGamal* yang menggabungkan keunggulan dari sistem kriptografi *ElGamal* yang dikonstruksikan oleh Marc Joye dan prinsip *general linear grup* pada matriks. Konsep dan penggunaan *general linear grup* akan dipelajari lebih mendalam dalam referensi aljabar linear dan terapan (Anton & Rorres, 2013; Hartanto et al., 2016; Lang, 1993).

B. Metode Penelitian

Penelitian ini merupakan jenis penelitian studi literatur. Berbagai sumber yang terdiri atas jurnal dan buku dikaji mendalam untuk mendapatkan ide dan referensi terbaik. Pustaka utama yang digunakan adalah jurnal *Secure ElGamal-type Cryptosystems Without Message Encoding* karya Marc Joye dan prosiding *Konstruksi Sistem Kriptografi Menggunakan General Linear Group* karya Ari Dwi Hartanto dan Diah Junia Eksi Palupi. Selanjutnya, salah satu bentuk konstruksi yang dikembangkan oleh Marc Joye akan dimodifikasi dengan konsep *General Linear Grup* dari pustaka kedua.

Adapun langkah yang dilakukan untuk mendukung penelitian ini adalah:

1. Mempelajari dan menganalisa jurnal *Secure ElGamal-type Cryptosystems Without Message Encoding* karya Marc Joye.

2. Mempelajari prosiding Konstruksi Sistem Kripto Menggunakan *General Linear Group* karya Ari Dwi Hartanto dan Diah Junia Eksi Palupi.
3. Menerapkan konsep general linear grup pada jurnal karya Marc Joye.
4. Menganalisa sifat-sifat khusus agar sistem kripto yang diusulkan bisa diterapkan sebagai suatu sistem yang lebih aman dari karya Marc Joye.

C. Hasil Dan Pembahasan

1. Sistem Kripto ElGamal Hasil Kontruksi Marc Joye

Sistem kripto *ElGamal* hasil kontruksi Marc Joye merupakan bentuk modifikasi dari sistem kripto *ElGamal* klasik. Sistem ini dimodifikasi dengan menambahkan proses verifikasi antara pihak pengirim dan pihak penerima informasi (pesan). Berikut ini algoritma pembangkit pasangan kunci:

1. Memilih generator h dan \bar{h} yang merupakan bilangan bulat (*integer*), kunci privat $\{z, \varepsilon, \bar{\varepsilon}\}$ dan bilangan prima p .
2. Membentuk $y = h^z \bmod p$ dan $x = h^\varepsilon \bar{h}^{\bar{\varepsilon}} \bmod p$. Perhatikan bahwa terdapat kunci publik $\{h, \bar{h}, p, y, x\}$ dan kunci privat $\{z, \varepsilon, \bar{\varepsilon}\}$.

Selanjutnya, penerima pesan akan mengirim kunci publik $\{h, \bar{h}, p, y, x\}$ ke pengirim pesan dan menyimpan kunci privat $\{z, \varepsilon, \bar{\varepsilon}\}$. Perlu diingat bahwa informasi yang dikirimkan berupa *plaintext* $m = \{1, 2, K, p\}$. Setelah kunci publik diterima oleh pengirim pesan maka dilakukan proses enkripsi, yaitu:

1. Memilih sebarang bilangan bulat (*integer*) r dan merahasiakannya.
2. Menghitung $c_1 = h^r \bmod p$, $\bar{c}_1 = \bar{h}^r \bmod p$ dan $c_2 = m y^r \bmod p$.
3. Membangkitkan kode verifikasi $v = x^r \bmod p$.

Pengirim pesan mengirimkan $\{c_1, \bar{c}_1, c_2, v\}$. Selanjutnya, penerima pesan dengan bantuan kunci privat melakukan verifikasi $v = c_1^\varepsilon \bar{c}_1^{\bar{\varepsilon}} \bmod p$. Jika v yang dikirimkan dan v yang dihitung sama maka dilanjutkan dengan menghitung $m = c_2 / c_1^z \bmod p$ (Joye, 2016).

2. General Linear Group

General Linear Group $GL(n, F_q)$ adalah himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga (*finite field*) F_q dengan determinan matriks tak nol. Secara matematis, dinotasikan $GL(n, F_q) = \{a_{ij} | \det \neq 0\}$ (Hartanto et al., 2016). Perhatikan bahwa F_q adalah suatu lapangan berhingga (*finite field*) yang memiliki q elemen. Pada penelitian ini, dipilih $F_q = \mathbb{F}_p$ sehingga diperoleh $GL(n, \mathbb{F}_p)$. Selanjutnya, banyaknya elemen (*order*

element) dari $GL(n, \phi_p)$ adalah
 $|GL(n, F_q)| = (q^n - 1)(q^{n-1} - q)K(q^n - q^{n-1}) = \prod_{k=0}^{n-1} (q^n - q^k)$. Misalkan dibentuk
 $GL(2, \phi_2)$ maka banyak anggota himpunan matriks adalah $(2^2 - 1)(2^2 - 2) = 6$
 yaitu $GL(2, \phi_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$. Perhatikan
 bahwa determinan dari matriks-matriks diatas tidak nol.

3. Matriks Sirkulan

Diberikan suatu matriks sirkulan A yaitu

$$A = \begin{bmatrix} a_0 & a_1 & K & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & K & a_{n-3} & a_{n-2} \\ M & M & O & M & M \\ a_2 & a_3 & K & a_0 & a_1 \\ a_1 & a_2 & K & a_{n-1} & a_0 \end{bmatrix}$$

Pada dasarnya, matriks sirkulan dibangun atas sebanyak n elemen pada suatu matriks sirkulan yang berukuran $n \times n$. Matriks sirkulan bersifat komutatif. Contoh matriks sirkulan yang paling sederhana adalah matriks identitas (Fan & Liu, 2018; Fuyong, 2011; KAYA, 2013)

4. Modifikasi Sistem Kripto ElGamal Yang Diusulkan

Pada kajian ini, kita akan menggunakan konsep matriks (*general linear group*) untuk menduplikasi modifikasi sistem kriptografi ElGamal hasil konstruksi Marc Joye. Misalkan diberikan sebarang matriks H dan \bar{H} serta dipilih sebarang bilangan bulat positif $z, \varepsilon, \bar{\varepsilon}$. Kita bentuk $Y = H^z \text{ mod } p$ dan $X = H^\varepsilon \bar{H}^{\bar{\varepsilon}} \text{ mod } p$, dengan p suatu bilangan prima. Jelas Y dan X juga berupa matriks yang berukuran sama dengan matriks H dan \bar{H} . Selanjutnya, dipilih sebarang bilangan bulat r dan dibentuk $C_1 = H^r \text{ mod } p$, $\bar{C}_1 = \bar{H}^r \text{ mod } p$, $C_2 = MY^r \text{ mod } p$. Kita juga harus memodifikasi $V = X^r \text{ mod } p$. Perhatikan bahwa berlaku

$$\begin{aligned} V &= X^r \text{ mod } p \\ &= (H^\varepsilon \bar{H}^{\bar{\varepsilon}})^r \text{ mod } p \\ &= \underbrace{(H^\varepsilon \bar{H}^{\bar{\varepsilon}})}_{r \text{ faktor}} \text{ mod } p \end{aligned}$$

Jika dipilih matriks H dan \bar{H} yaitu matriks-matriks yang komutatif maka diperoleh persamaan ,

$$\begin{aligned}
 V &= \left(\underset{r \text{ faktor}}{\begin{pmatrix} H^\varepsilon & K & H^\varepsilon \\ 1 & 4 & 2 \\ & 4 & 3 \end{pmatrix}} \right) \left(\underset{r \text{ faktor}}{\begin{pmatrix} \bar{H}^{\bar{\varepsilon}} & K & \bar{H}^{\bar{\varepsilon}} \\ 1 & 4 & 2 \\ & 4 & 3 \end{pmatrix}} \right) \text{ mod } p \\
 &= (H^\varepsilon)^r (\bar{H}^{\bar{\varepsilon}})^r \text{ mod } p \\
 &= (H^r)^\varepsilon (\bar{H}^r)^{\bar{\varepsilon}} \text{ mod } p \\
 &= C_1^\varepsilon \bar{C}_1^{\bar{\varepsilon}} \text{ mod } p
 \end{aligned}$$

Pada bagian akhir, dibentuk

$$\begin{aligned}
 \frac{C_2}{C_1^z} \text{ mod } p &= C_2 C_1^{-z} \text{ mod } p \\
 &= C_2 (C_1^z)^{-1} \text{ mod } p \\
 &= M Y^r (H^{rz})^{-1} \text{ mod } p \\
 &= M (H^{rz}) (H^{rz})^{-1} \text{ mod } p \\
 &= M
 \end{aligned}$$

Pada kajian ini, kita diharuskan menggunakan matriks H yang mempunyai invers (*invertible*) pada modulo p serta memiliki sifat komutatif. Dengan demikian, dipilih matriks H dan \bar{H} yang merupakan matriks sirkulan. Jelas bahwa syarat utama modifikasi sistem kriptografi *ElGamal* ini bekerja dengan baik, jika matriks H dan \bar{H} merupakan matriks sirkulan yang memiliki invers atas modulo p . Jadi, diperlukan bentuk khusus dari konsep *general linear group* yaitu matriks sirkulan yang berlaku konsep *general linear group*. Berikut ini, algoritma untuk modifikasi sistem kriptografi yang diusulkan:

Algoritma pembentuk pasangan kunci

1. Memilih generator matriks H dan \bar{H} yang merupakan matriks sirkulan yang memiliki invers atas modulo p , kunci privat $\{z, \varepsilon, \bar{\varepsilon}\}$ dan bilangan prima p .
2. Membentuk $Y = H^z \text{ mod } p$ dan $X = H^\varepsilon \bar{H}^{\bar{\varepsilon}} \text{ mod } p$. Perhatikan bahwa terdapat kunci publik $\{H, \bar{H}, p, Y, X\}$ dan kunci privat $\{z, \varepsilon, \bar{\varepsilon}\}$.

Enkripsi

1. Memilih sebarang r suatu bilangan bulat (*integer*) dan merahasiakannya.
2. Menghitung $C_1 = H^r \text{ mod } p$, $\bar{C}_1 = \bar{H}^r \text{ mod } p$ dan $c_2 = M Y^r \text{ mod } p$.
3. Membangkitkan kode verifikasi $V = X^r \text{ mod } p$.

Deskripsi

1. Memverifikasi $V = C_1^\varepsilon \bar{C}_1^{\bar{\varepsilon}} \text{ mod } p$.
2. Jika V yang dikirimkan dan V yang dihitung sama maka dilanjutkan dengan menghitung $M = C_2 C_1^{-z} \text{ mod } p$.

5. Keunggulan Modifikasi Sistem Kripto ElGamal Yang Diusulkan

Pada sistem kripto *ElGamal* hasil kontruksi Marc Joye, *plaintext* m berbentuk integer. Jika diberikan pesan $M = \{m_1, m_2, K, m_n\}$ maka proses enkripsi dan deskripsi ada sebanyak n proses. Pada modifikasi sistem kripto *ElGamal* yang diusulkan, pesan $M = \{m_1, m_2, K, m_n\}$ diblok berdasarkan ukuran matriks yang dikehendaki. Jika dibentuk kedalam matriks berukuran $k \times k$

dan $k < m$ maka diperoleh $M_1 = \begin{bmatrix} m_1 & K & m_k \\ M & O & M \\ m_l & K & m_{kk} \end{bmatrix}$. Misalkan ada *plaintext*

$M = 12-3-4-6-7-1-11$ dan dipilih $M_{2 \times 2}$ diperoleh $M_1 = \begin{bmatrix} 12 & 3 \\ 4 & 6 \end{bmatrix}$ dan

$M_2 = \begin{bmatrix} 7 & 1 \\ 11 & 8 \end{bmatrix}$. Perhatikan bahwa entri 8 pada matriks M_2 merupakan *elemen*

dummy, yang digunakan untuk melengkapi entri elemen pada matriks. *Elemen dummy* boleh dipilih sebarang. Dengan demikian, pembuatan blok-blok *plaintext* akan membuat *ciphertext* semakin acak. Jadi, modifikasi sistem kripto *ElGamal* yang diusulkan akan lebih aman terhadap serangan (*attack*).

6. Contoh Kasus

Misalkan Bob akan berkirim pesan kepada Alice. Sebagai penerima pesan, Alice bertugas untuk membangkitkan pasangan kunci yang digunakan untuk enkripsi dan deskripsi.

Algoritma pembangkit pasangan kunci

Alice membangkitkan pasangan kunci dengan memilih matriks-matriks sirkulan $H = \begin{bmatrix} 1 & 7 \\ 7 & 1 \end{bmatrix}$ dan $\bar{H} = \begin{bmatrix} 11 & 13 \\ 13 & 11 \end{bmatrix}$ serta memilih bilangan bulat $p = 2357$,

$z = 123$, $\varepsilon = 512$, $\bar{\varepsilon} = 709$. Alice menghitung nilai $Y = H^z \text{ mod } p = \begin{bmatrix} 554 & 2212 \\ 2212 & 554 \end{bmatrix}$

dan $X = H^\varepsilon \bar{H}^{\bar{\varepsilon}} \text{ mod } p = \begin{bmatrix} 86 & 1431 \\ 1431 & 86 \end{bmatrix}$. Dengan demikian, diperoleh kunci publik

$$\left\{ H = \begin{bmatrix} 1 & 7 \\ 7 & 1 \end{bmatrix}, \bar{H} = \begin{bmatrix} 11 & 13 \\ 13 & 11 \end{bmatrix}, p = 2357, Y = \begin{bmatrix} 554 & 2212 \\ 2212 & 554 \end{bmatrix}, X = \begin{bmatrix} 86 & 1431 \\ 1431 & 86 \end{bmatrix} \right\}$$

dan kunci privat $\{z = 123, \varepsilon = 512, \bar{\varepsilon} = 709\}$. Selanjutnya, Alice mengirim kunci publik ke Bob.

Enkripsi

Bob menerima kunci publik dari Alice. Bob memilih $r = 451$ dan merahasiakannya. Selanjutnya, Bob menghitung nilai

$C_1 = H^r \bmod p = \begin{bmatrix} 1163 & 616 \\ 616 & 1163 \end{bmatrix}$, $\bar{C}_1 = \bar{H}^r \bmod p = \begin{bmatrix} 1926 & 2054 \\ 2054 & 1926 \end{bmatrix}$. Misalkan Bob akan mengirim pesan dengan kode ASCII “123435783341204343”. Perhatikan bahwa matriks H dan \bar{H} berukuran 2×2 sehingga dibentuk *plaintext* $M_1 = \begin{bmatrix} 123 & 435 \\ 783 & 341 \end{bmatrix}$ dan $M_2 = \begin{bmatrix} 204 & 343 \\ 111 & 111 \end{bmatrix}$. Pada matriks M_2 terdapat entri elemen dummy 1. Selanjutnya Bob menghitung $(C_2)_i = M_i Y^r \bmod p$, dengan $i=1,2$ sehingga diperoleh $(C_2)_1 = \begin{bmatrix} 1066 & 1255 \\ 2179 & 1322 \end{bmatrix}$ dan $(C_2)_2 = \begin{bmatrix} 747 & 2259 \\ 373 & 373 \end{bmatrix}$. Bob juga menghitung kode verifikasi $V = X^r \bmod p = \begin{bmatrix} 1815 & 2209 \\ 2209 & 1815 \end{bmatrix}$. Selanjutnya, Bob mengirim

$$\left\{ \begin{array}{l} C_1 = \begin{bmatrix} 1163 & 616 \\ 616 & 1163 \end{bmatrix}, \bar{C}_1 = \begin{bmatrix} 1926 & 2054 \\ 2054 & 1926 \end{bmatrix}, (C_2)_1 = \begin{bmatrix} 1066 & 1255 \\ 2179 & 1322 \end{bmatrix}, \\ (C_2)_2 = \begin{bmatrix} 747 & 2259 \\ 373 & 373 \end{bmatrix}, V = \begin{bmatrix} 1815 & 2209 \\ 2209 & 1815 \end{bmatrix} \end{array} \right\}$$

kepada Alice.

Deskripsi

Alice memverifikasi kode $V = C_1^e \bar{C}_1^{\bar{e}} \bmod p = \begin{bmatrix} 1815 & 2209 \\ 2209 & 1815 \end{bmatrix}$. Perhatikan bahwa nilai matriks V yang dikirimkan Bob sama dengan matriks V yang dihitung Alice. Dengan demikian, Alice melanjutkan menghitung $M_i = (C_2)_i C_1^{-z} \bmod p$ untuk $i=1,2$. Alice memperoleh $M_1 = \begin{bmatrix} 123 & 435 \\ 783 & 341 \end{bmatrix}$ dan $M_2 = \begin{bmatrix} 204 & 343 \\ 111 & 111 \end{bmatrix}$. Jadi, Alice mendapatkan pesan yang sama dari Bob yaitu “123435783341204343” dengan tambahan pesan dummy “111111”.

D. Simpulan

Modifikasi sistem kriptografi *ElGamal* yang diusulkan merupakan proses duplikasi sistem kriptografi yang dikerjakan oleh Marc Joye. Pada sistem ini, generator dibangkitkan dengan matriks sirkular yang memiliki invers (*invertible matrix*) atas modulo p yang merupakan bentuk khusus dari konsep *general linear group*. Keuntungan modifikasi sistem kriptografi *ElGamal* yang diusulkan adalah *ciphertext* yang dihasilkan menjadi lebih acak karena operasi perpangkatan pada matriks. Jadi, tingkat keamanan yang dihasilkan menjadi lebih baik dari sistem kriptografi *ElGamal* hasil konstruksi Marc Joye.

E. Daftar Pustaka

- Anton, H., & Rorres, C. (2013). *Elementary Linear Algebra: Applications Version, 11th Edition*. Wiley eGrade.
- Bharathi, C. R. (2018). Improved ELGAMAL Encryption for Elliptic Curve Cryptography. *International Journal of Pure and Applied Mathematics*, 118(17), 341–353.
- Boruah, D., & Saikia, M. (2015). Implementation of ElGamal Elliptic Curve Cryptography over prime field using C. In *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014*. <https://doi.org/10.1109/ICICES.2014.7033751>
- ElGamal, T. (1985). A Public Key Cryptosystem and A Signature Based on Discrete Logarithms. *IEEE Transaction on Information Theory*, 31(4), 469–472.
- Fan, Y., & Liu, H. (2018). Double circulant matrices. *Linear and Multilinear Algebra*, 66(10), 2119–2137. <https://doi.org/10.1080/03081087.2017.1387513>
- Fang, J., Liu, C., & Wu, J. (2016). Weakness of an ElGamal-like cryptosystem for enciphering large messages. In *Lecture Notes in Electrical Engineering* (Vol. 375, pp. 1225–1231). https://doi.org/10.1007/978-981-10-0539-8_126
- Fu, M., & Chen, W. (2010). Elliptic curve cryptosystem ElGamal encryption and transmission scheme. In *ICCASM 2010 - 2010 International Conference on Computer Application and System Modeling, Proceedings* (Vol. 6). <https://doi.org/10.1109/ICCASM.2010.5620105>
- Fun, T. S., & Samsudin, A. (2018). An Efficient ElGamal Encryption Scheme Based on Polynomial Modular Arithmetic in F_2^n . In *Lecture Notes in Electrical Engineering* (Vol. 488, pp. 99–107). https://doi.org/10.1007/978-981-10-8276-4_10
- Fuyong, L. (2011). The inverse of circulant matrix. *Applied Mathematics and Computation*, 217(21), 8495–8503. <https://doi.org/10.1016/j.amc.2011.03.052>
- Hartanto, A. D., Junia, D., & Palupi, E. (2016). Konstruksi Sistem Kripto Menggunakan General Linear Group. *Prosiding Seminar Nasional Aljabar USD 2016*, 203–214.
- Joye, M. (2016). Secure ElGamal-Type cryptosystems without message encoding. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9100, 470–478. https://doi.org/10.1007/978-3-662-49301-4_29
- Kaya, E. (2013). On Circulant Matrices. *Communications, Faculty Of Science, University of Ankara Series A1 Mathematics and Statistics*, (January 2004), 015–024. https://doi.org/10.1501/commua1_0000000593
- Lang, S. (1993). *Linear Algebra*. New York: Springer.
- Mahalanobis, A. (2012). A Simple Generalization of the ElGamal Cryptosystem to Non-Abelian Groups II. *Communications in Algebra*, 40(9), 3583–3596. <https://doi.org/10.1080/00927872.2011.602998>
- Mandangan, A., Yin, L. S., Hung, C. E., & Hussin, C. H. C. (2014). ElGamal

- cryptosystem with embedded compression-crypto technique. In *AIP Conference Proceedings* (Vol. 1635, pp. 455–460).
<https://doi.org/10.1063/1.4903621>
- Murakami, Y., & Kasahara, M. (2015). Hybrid inter-organization cryptosystem using ElGamal cryptosystem. In *2015 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2015* (pp. 378–379).
<https://doi.org/10.1109/ICCE-TW.2015.7216953>
- Rao, F.-Y. (2017). On the Security of a Variant of ElGamal Encryption Scheme. *IEEE Transactions on Dependable and Secure Computing*, 14(8), 1–1.
<https://doi.org/10.1109/TDSC.2017.2707085>
- Sharma, P., Sharma, S., & Dhakar, R. S. (2011). Modified Elgamal Cryptosystem Algorithm (MECA). In *2011 2nd International Conference on Computer and Communication Technology, ICCCT-2011* (pp. 439–443).
<https://doi.org/10.1109/ICCCT.2011.6075141>
- Yang, C.-C., Chang, T.-Y., Li, J.-W., & Hwang, M.-S. (2003). Simple Generalized Group-Oriented Cryptosystems Using ElGamal Cryptosystem. *Informatica*, 14(1), 111–120.